Technical Cybersecurity

External Exploits

Stereotypical Hacker

External exploits are the most exciting

- …and least used.

Hacking a company from your living room

- Or wherever, but you get the idea.
- Attack a company from the outside
- Probably the hardest to pull off

Device Flaws

Typical exploitable flaws include

- Buffer overflows
- Memory allocation errors
- Insufficient credential checking
- Web-based flaws

Remote code execution

- You're getting code onto a system and getting it to run

Case: CVE-2018-6789

Flaw in Exim SMTP Listener

- Message transfer agent
- https://www.exim.org
- Transfers email from one system to another

Error in base64 decoding

- Error decoding base64 encoded strings
- binary -> text encoding
- Allows binary data to be sent in email without being interpreted inadvertently

Case: CVE-2018-6789

Exploitation process

- Put together a special treat as a message
- Send the message
- Profit!

Details?

- See the exploit: https://www.exploit-db.com/exploits/45671/

How about another?

Case: CVE-2018-10933

Flaw in libssh

- Common library used to implement SSH functionality
- Multiplatform, implements SSHv2
- https://www.libssh.org

Error in internal state machine

- Flaw in the design of the state machine that implements authentication
- Allows attackers to authenticate by transmitting a SUCCESS message instead of a REQUEST

Case: CVE-2018-10933

Exploitation process

- Connect to a server using libssh
- Present an out-of-order message to bypass credential processing

Details?

- https://www.exploit-db.com/exploits/45638/

There are many of these, but they tend to get patched quickly.

What about things that don’t?